WHAT IS CLAIMED IS:

1. A Gigabit Ethernet-based passive optical network comprising:

an OLT for receiving a public key through a transmission medium, encrypting a secret key by means of the received public key, transmitting the encrypted secret key, encrypting data by means of the secret key, and transmitting the encrypted data, the OLT being located in a service provider-side; and

an ONT for transmitting the public key to the OLT, receiving the secret key transmitted from the OLT, decrypting the secret key by means of a private key, receiving the data, and decrypting the received data by means of the decrypted the secret key,

wherein the public key is used for encrypting the secret key, the secret key is encrypted by means of the public key, and the data is encrypted by the OLT by means of the secret key.

2. The Gigabit Ethernet-based passive optical network as claimed in claim 1, wherein the OLT comprises:

a GE-PON OLT MAC module for transmitting input data to a predetermined path;

a GMII module for providing an interface between a transmission medium and the GE-PON OLT MAC module;

an OLT key management unit for managing a public key transmitted from the ONT and a secret key for encrypting the data; and

a data encryption unit for encrypting the data by means of the secret key.

3. The Gigabit Ethernet-based passive optical network as claimed in claim 2, wherein the GMII module comprises:

a PCS module for selectively encoding or decoding input blocks of data and outputting the encoded data or the decoded data;

a PMA module for selectively performing a serial conversion or a parallel conversion with respect to input data and outputting the converted data; and

a PMD module for converting electrical signals, which are data output from the PMA module, into optical signals, transmitting the optical signals to the transmission medium, converting optical signals received through the transmission medium 300 into electrical signals, and transmitting the electrical signals to the PMA module.

4. The Gigabit Ethernet-based passive optical network as claimed in claim 2, wherein the OLT key management unit comprises:

a public key storage unit for storing a public key transmitted from the ONT;

a secret key generation unit for generating a secret key for encrypting the data when the public key is stored in the public key storage unit; and

a secret key encryption unit for encrypting the secret key generated by secret key generation unit by means of the public key stored in the public key storage unit.

5. The Gigabit Ethernet-based passive optical network as claimed in claim 1, wherein the ONT comprises:

a GE-PON OLT MAC module for transmitting input data to a predetermined path;

a GMII module for providing an interface between a transmission medium and the GE-PON OLT MAC module;

an ONT key management unit for managing a public key and a private key and decrypting the encrypted data transmitted from the OLT by means of the private key; and

a data decryption unit for decrypting the encrypted data transmitted from the OLT by means of the secret key decrypted by the OLT key management unit.

6. The Gigabit Ethernet-based passive optical network as claimed in claim 5, wherein the GMII module comprises:

a PCS module for selectively encoding or decoding input blocks of data and outputting the encoded data or the decoded data;

a PMA module for selectively performing a serial conversion or a parallel conversion with respect to input data and outputting the converted data; and

a PMD module for converting electrical signals, which are data output from the PMA module, into optical signals, transmitting the optical signals to the transmission medium, converting optical signals received through the transmission medium 300 into electrical signals, and transmitting the electrical signals to the PMA module.

7. The Gigabit Ethernet-based passive optical network as claimed in claim 1,

wherein the ONT key management unit comprises:

a public key storage unit for storing the public key;

a private key storage unit for storing the private key; and

a secret key decryption unit for decrypting the encrypted secret key transmitted from the OLT by means of the secret key stored in the private key storage unit, and outputting the decrypted secret key to the data decryption unit.

8. The Gigabit Ethernet-based passive optical network as claimed in claim 1, wherein the public key and the private key are respectively a RSA public key and a RSA private key.

9. The Gigabit Ethernet-based passive optical network as claimed in claim 1, wherein the secret key is an AES secret key.

10. An encryption method for transferring data between an OLT and a plurality of ONTs in an E-PON structure, the encryption method comprising the steps of:

a) transmitting, by the ONT, a public key to the OLT;

b) encrypting, by the OLT, a secret key by means of the public key transmitted from the ONT and transmitting the encrypted secret key to the ONT;

c) decrypting, by the ONT, the encrypted secret key transmitted from the OLT by means of a private key;

d) encrypting, by the OLT, data by means of the secret key and transmitting the

encrypted data to the ONT; and

e) decrypting, by the ONT, the encrypted data transmitted from the OLT by means of the decrypted secret key.

11. The encryption method as claimed in claim 10, wherein step b) comprises:

b-1) storing the public key transmitted from the ONT;

b-2) generating a secret key for encrypting the data when the public key is stored;

b-3) encrypting the secret key by means of the public key; and

b-4) transmitting the encrypted secret key to the ONT.

12. An encryption method for transferring data between an OLT and a plurality of ONTs in an E-PON structure, the encryption method comprising the steps of:

a) transmitting, when power is turned on and the OLT is driven, gate signals to the ONTs in order to detect ONTs connected through a transmission medium;

b) transmitting, by the ONTs, registration requirement signals and RSA public keys corresponding to the gate signals;

c) registrating, by the OLT, the ONTs in accordance with the registration requirement signals transmitted from the ONTs, assigning LLIDs with respect to the ONTs, and transmitting information for the assignment to the ONTs;

d) encrypting, by the OLT, secret keys by means of the public keys and transmitting the encrypted secret keys to the ONTs;

e) decrypting, by the ONTs, the encrypted secret keys transmitted from the OLT by

means of private keys;

f) confirming, by the OLT and the ONTs, mutual sharing of the public keys and the secret keys, the OLT assigning bandwidths necessary for data transmission to the ONTs;

g) encrypting, by the OLT, data by means of the secret keys and transmitting the encrypted data to the ONTs; and

h) decrypting, by the ONTs, the encrypted data transmitted from the OLT by means of the decrypted secret keys.

13. An encryption method for transferring data by an OLT in an E-PON structure, the encryption method comprising the steps of:

a) receiving a public key;

b) encrypting a secret key using the public key

c) transmitting the encrypted secret key;

d) encrypting data using the secret key; and

e) transmitting the encrypted data .

14. The encryption method as claimed in claim 13, wherein step b) comprises:

b-1) storing the public key transmitted;

b-2) generating a secret key for encrypting the data when the public key is stored; and

b-3) encrypting the secret key by means of the public key.

15. An encryption method for transferring data by an OLT in an E-PON structure, the encryption method comprising the steps of:

transmitting, when power is turned on and the OLT is driven, gate signals through a transmission medium;

receiving registration requirement signals and RSA public keys corresponding to the gate signals;

registrating the received registration requirement signals,

assigning respective LLIDs;

transmitting information for the assignment;

encrypting secret keys by means of the public keys and transmitting the encrypted secret keys;

confirming mutual sharing of the public keys and the secret keys;

assigning bandwidths necessary for data transmission;

encrypting data using the secret keys; and

transmitting the encrypted data.